IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	
	)	Criminal No. 1:16-cr-42
ARDIT FERIZI,	)	
	)	
Defendant.	)	

Government's Response to Court's Order

The defendant, Ardit Ferizi, is a Kosovo citizen, computer hacker, and sympathizer of the Islamic State of Iraq and al-Sham (ISIS). Ferizi was convicted in 2016 of providing material support to ISIS and unauthorized computer access. Ferizi breached the servers of a U.S. company, stole personal identifying information of over 100,000 of its customers, and used that information to specifically locate U.S. military and government personnel. He identified approximately 1,300 such individuals and sent the information to a high-profile ISIS member in Syria, intending for ISIS to "hit them hard." Soon after, the ISIS member published a "kill list" with these names on Twitter, adding the following message: "the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!"

In sentencing Ferizi to 240 months' imprisonment in 2016, the Court rejected his attempts to excuse his conduct, accepted the Presentence Investigation Report's conclusion that he provided material support with the intent, knowledge, or reason to believe it would be used to commit or assist in the commission of a violent act, and rejected the theory that Ferizi's crimes should be treated less seriously because his victims did not suffer physical harm.

In August 2020, the Court denied Ferizi' first motion for compassionate release. In doing so, the Court repeatedly recognized that Ferizi was too dangerous to release and that doing so

would not protect the safety of the community from future hacking. In December 2020, the Court granted the defendant's motion for compassionate release. In doing so, the Court rejected the government's arguments that releasing Ferizi to a foreign country would not protect the public from further crimes of the defendant.

The government appealed the Court's release order and about one month later, Ferizi was charged with new crimes in the Northern District of California. These new charges stemmed from Ferizi's conduct while in prison on his convictions in this case. After hearing oral argument, the Fourth Circuit remanded back to this Court to consider the new charges.

As explained in greater detail below, the new charges are but the latest chapter in Ferizi's career of crime and deception. As with his prior offenses, Ferizi is again accused of a crime involving the theft of innocent victims' personal identifying information. Ferizi's background, history, and skillset made him an inappropriate candidate for compassionate release in December 2020. The government has consistently articulated this position. The new charges only confirm that point.

Procedural History

A. Ferizi's Offense Conduct

On September 21, 2014, ISIS' spokesperson, Abu Muhammad al-Adnani, openly called for attacks against citizens and military employees of countries participating in the U.S.-led coalition against ISIS. (ECF No. 36 at 2.) On March 20, 2015, ISIS member Junaid Hussain, acting under the banner of "the Islamic State Hacking Division," posted online a "kill list" that included 100 names and addresses of U.S. military personnel. *Id*. Hussain was a Syria-based ISIS member

actively engaged in supporting the group's efforts to conduct terrorist attacks against U.S. military members and government personnel. *Id*. at 4.[1]

About one month later, Ferizi, then-residing in Malaysia and using the Twitter moniker "@Th3Dir3ctorY," began communicating with an ISIS member known as Tariq Hamayun. (ECF No. 36 at 3.) Hamayun used the Twitter moniker "@Muslim_Sniper_D." (PSR ¶ 11.) On April 21, 2015, Hamayun tweeted as follows: "God Willingly will be making the best Electronics LAB in the Islamic state, would be producing sophisticated IEDS." (ECF No. 2 at 10.) The next day, Hamayun, using the same account, tweeted that "IEDs is my favorite weapon after Sniping, u hit the enemy & disappear in thin air like a Ghost. Its a Must." *Id*. On April 26-27, 2015, Ferizi and Hamayun communicated through Twitter. (ECF No. 2 at 10; ECF No. 36 at 3.) At one point, Ferizi told Hamayun that he had "4 million data of kuffar countrys which attacking islamic state." (ECF No. 54-1 at 7.) Ultimately, Ferizi provided Hamayun with screenshots of credit card information belonging to 68 individuals. (PSR ¶ 11; ECF No. 36 at 3.) Later, Hamayun commented on this information, "MashAllah [what God has willed] brother I check some of this info its really good[,]" and added, "Can do some damage inshallah[.]" (ECF No. 54-1 at 7.) Ferizi asked Hamayun to confirm his identity as "Abu Al-Britani," whom he knew to be an ISIS member. (PSR ¶ 11.) Hamayun confirmed his identity and association with Junaid Hussain, claiming that Hussain "told me a lot about u." (PSR ¶ 11; ECF No. 54-1 at 7.) Hamayun also implored Ferizi to "come

[1] The Junaid Hussain referenced herein is the same Hussain who has figured prominently in other recent prosecutions, such as the plot to fulfill an ISIS fatwa by killing American activist and commentator Pamela Geller. *See United States v. Wright*, 937 F.3d 8 (1st Cir. 2019); *see also United States v. Mumuni Saleh*, 946 F.3d 97, 102 (2d Cir. 2019) ("Mumuni was offered a pressure-cooker bomb from Saleh for his attack. When Mumuni asked Saleh whether it would be permissible from a religious standpoint to die during his attack on law enforcement, Saleh contacted Junaid Hussain ("Hussain"), a notorious Syria-based ISIS attack facilitator. Hussain expressly authorized Mumuni's suicide attack").

and join us in the Islamic state." "InshAllah," or God-willing, Ferizi responded. (ECF No. 54-1 at 7.)

Beginning in June 2015, Ferizi unlawfully accessed the Arizona-based server of a U.S. company. (ECF No. 36 at 3.) Ferizi obtained administrator-level access and spent the next two months extracting the personal identifying information (PII) of over 100,000 customers. *Id*. Ferizi specifically searched for email addresses ending in ".gov" or ".mil." and thereby culled the PII of approximately 1,300 U.S military and government personnel. *Id*.

Ferizi then provided the information to ISIS "with the understanding that ISI[S] would use the PII to hit them hard." *Id*. at 4. Ferizi did this by contacting Junaid Hussain, whom he knew was a member of ISIS actively engaged in supporting the group. *Id*. at 3–4. At one point, Hussain told Ferizi: "we will make like a message inshAllah […] like u know the hit list I made […] we will make message to kuffar and release the .mil and .gov[.]" (ECF No. 54-1 at 10–11.) Soon after, Hussain stated "Allahu Akbar [...] Akhi this will hit them hard[.]" *Id*. at 11. Ferizi immediately responded "yes brother inshalllah[.]" *Id*.[2]

On August 11, 2015, Hussain, acting in the name of "the Islamic State Hacking Division," issued a public message over Twitter with the heading: "NEW: U.S. Military AND government HACKED by the Islamic State Hacking Division!" (ECF No. 36 at 4–5; ECF No. 2 at 12.) The

[2] Earlier in the conversation, a similar exchange ensued:

> Ferizi: there is a huge db [database]
> Hussain: Allahu Akbar
> Hussain: we need to hit them hard
> Ferizi: yes, inshaAllah
> Hussain: ok akhi we will release biidnillah
> Ferizi: just when we hit hit them strong

(ECF No. 54-1 at 9.)

message contained a link to a 30-page document containing the names, e-mail addresses, passwords, locations, and telephone numbers of the 1,300 U.S. military members and government personnel Ferizi had unlawfully obtained. The document, addressed to the "Crusaders" conducting "bombing campaign[s] against the muslims," stated as follows:

> we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!

(ECF No. 36 at 4–5.) About two weeks later, Hussain was killed by an airstrike in Syria.

On October 6, 2015, Ferizi was charged by criminal complaint in the Eastern District of Virginia. Malaysian authorities arrested him on October 12, 2015, and extradited him to the U.S. on January 22, 2016.[3]

B. Ferizi is indicted, pleads guilty, and receives a 240-month sentence.

On February 16, 2016, Ferizi was charged in a four-count indictment with: conspiring to provide and providing material support and resources to a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B (Counts One and Two); unauthorized computer access, in violation of 18 U.S.C. §§ 1030(a)(2)(c), (c)(2)(B)(ii) (Count Three); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(2).

[3] During the relevant period, Ferizi sought to aid or promote ISIS in several other ways. For example, he administered a website that hosted dozens of ISIS videos. (ECF No. 54-1 at 3–5.) He directed an offer of technical assistance at three now-suspended pro-ISIS Twitter accounts, stating as follows: "brother wait till im making the script which u can upload and never get deleted (DEDICATED SERVERS)[.]" (ECF No. 2 at 13–14.) And in private internet chats, he defended ISIS' release of hit lists containing U.S. service members' information ("cos they was the people who killed people in iraq and syria [...] if someone kill your family and run would u not find him and kill him?"), and the group's highly publicized beheadings of civilians ("ill tell u they never kill someone without reasons believe me i guarantee u[.]"). (ECF No. 54-1 at 7.)

On June 15, 2016, Ferizi pled guilty to Counts Two and Three of the indictment. As part of his plea, Ferizi agreed that "[d]uring this entire period of the [charged conduct], [he] knew ISIS had engaged in and was engaging in terrorist activity and terrorism." (ECF No. 36 at 3.) Ferizi agreed that his actions "were done willfully and knowingly and with the specific intent to violate the law, and were not committed by mistake, accident, or other innocent reason." *Id*. at 3, 5. He further admitted that he provided ISIS with the PII with the understanding that ISIS would use the PII to "hit them hard." *Id*. at 4.[4] In pleading guilty to Count Three, Ferizi necessarily admitted that he intentionally accesses the victim company's server without authorization and that he did so in furtherance of the material support violation. *See* § 1030(a)(2)(C), (c)(2)(B)(ii). In other words, Ferizi admitted that he hacked the victim company to promote, advance, or further the material support violation. Ferizi also stipulated to the application of a 12-level upward adjustment under U.S.S.G. § 3A1.4 because his material support offense was a felony involving a federal crime of terrorism under 18 U.S.C. § 2332b(g)(5)(A). (ECF No. 35 at 3–4.) In doing so, Ferizi necessarily accepted that he had "the specific intent required by the terrorism enhancement." *United States v. Chandia*, 675 F.3d 329, 331 (4th Cir. 2012). Namely, that his material support offense was "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct." § 2332b(g)(5).

Prior to sentencing, the Office of Probation prepared a Presentence Investigation Report (PSR). As calculated by the PSR, Ferizi's Guideline range was 360 months to life imprisonment, capped at the 300-month combined statutory maximum. As relevant here, the PSR recommended the additional application of a two-level base offense increase under U.S.S.G. § 2M5.3(b)(1)(E) for the provision of material support with the intent, knowledge, or reason to believe it would be

[4] As he himself put it, "just when we hit hit them strong." (ECF No. 54-1 at 9.)

used to commit or assist in the commission of a violent act. (PSR ¶ 30.) Ferizi objected to the application of § 2M5.3(b)(1)(E) but Probation insisted on its applicability:

> The defendant sought to obtain the personal information of specific individuals for ***the sole purpose*** of providing their information to ISIL, knowing ISIL had targeted that very group as a group to be harmed. As detailed in the Statement of Facts, in June of 2015, the defendant reached out to an individual he knew to be a terrorist and provided him with the personal information of United States military and government personnel. He was aware the individual and his ISIL colleagues were exerting efforts to conduct violent attacks against United States military and government personnel. He also knew that ISIL planned to "hit them hard."
>
> The guideline applications use a preponderance standard, and this officer believes it is more likely than not that the defendant deliberately sought the victims' information knowing ISIL members would use it to engage in acts of violence against them.

(PSR p.18–19) (Addendum) (emphasis added). In his sentencing submission, Ferizi continued to object to the application of the enhancement, arguing that he did not intend to "bring violence to anyone" but was instead merely "boast[ing] about his hacking exploits on-line[.]" (ECF No. 53 at 4.) The Court subsequently "accept[ed] the guidelines as they've been calculated, because I think they are correct given the facts of this case." (ECF No. 77 at 27.)

At sentencing, on September 23, 2016, the Court offered Ferizi an opportunity to allocute. After an allocution comprising four lines of transcript text, the Court asked Ferizi if he had "any true understanding of what [he] actually did[.]" (ECF No. 77 at 25.) Ferizi claimed he did, to which the Court responded "I'm still not sure. Why did you do it?" *Id*. Ferizi then claimed that "it was something -- happened very fast." *Id*. Unpersuaded, the Court responded as follows: "It didn't happen that fast. You're communicating back and forth over a period of time, aren't you?" *Id*. Ferizi responded by mentioning a girl he met online who supported ISIS. *Id*. To this, the Court responded as follows: "Well, this was a case where it wasn't a one time incident. You had plenty of time to think about what was going on." *Id*.

Prior to and during sentencing, Ferizi made several such attempts at justifying or explaining his actions. On this issue, however, neither Ferizi nor defense counsel could get their story straight. Prior to sentencing, Ferizi claimed that he transferred the PII to ISIS to "show off his hacking skills to people he met online." (PSR ¶ 27.) (He made this claim despite clearly agreeing with Junaid Hussain that they would release the PII anonymously, despite admitting that his actions were not committed for any "innocent reason," despite admitting that he hacked to further the material support violation, and despite stipulating under § 3A1.4(a) that his motive in providing material support was to influence or affect government conduct by intimidation or coercion, or to retaliate against government conduct.) But in Ferizi's sentencing submission, defense counsel offered another explanation: Ferizi did what he did to get back at the U.S. for not removing an article published online about his activities. As defense counsel put it: "Motivated by his wholly misguided and immature desire to respond to the perceived slight, Mr. Ferizi broke into a retail database in the United States and extracted emails and passwords that appeared to belong to government or military employees. He then sent Hussain the link containing information he had culled from the retail database." (ECF No. 53 at 86.) At sentencing, defense counsel doubled down on the "smear post" theory, arguing that Ferizi committed his crimes to "get back at the United States Embassy for not removing the smear post" and "that that truly is his explanation for what he did." (ECF No. 77 at 20.) Yet in his forensic psychological evaluation, Ferizi was more candid. There, Ferizi "reported that hacking gave him a sense of control and power that he liked and that this feeling was at least initially a primary motivator for hacking activities." (Report at 5). Ferizi also admitted that he viewed his hacking activities as morally justified. *Id*. at 6.[5] Ferizi explained

[5] Ferizi also "stated that while he had many associates who hacked for criminal profit (*e.g.*, ransoming fixes for viruses they planted), he did not engage in such activity." (p.6). This was a lie. Ferizi did just that in *this* case when he attempted to extort a bitcoin ransom from the victim

that he later used hacking as a way of challenging governments. *Id*. at 5. Ferizi also explained that his focus shifted to the U.S. because of its technological advancement and that his hacking aimed at "proving that [his] theories about government are correct." *Id*.

At sentencing, Ferizi attempted to minimize the level of harm suffered by the 1,300 victims whose PII was released on the internet. The crux of Ferizi's argument on this score was that none of his victims were physically harmed. (*See* ECF No. 53 at 7 ("[N]o one was physically harmed as a result of Mr. Ferizi's conduct."); 18 ("[T]here was not a physical attack on the victims"); (ECF No. 77 at 22) (defense counsel distinguishing case from *Adam Chesser* prosecution).) But the Court rejected these arguments. As the Court stated, "although the defense has argued that the victims are not victims as -- as much as in the other case that the Government has cited, just having your name on a list knowing that you've been identified to a terrorist group, in my view, is sufficiently terrorizing for those people on the list. And their letters certainly attest to that fact." (ECF No. 77 at 27.) Continuing, the Court added that one victim "who has a very unique name, in particular, mentions that maybe the only name in that particular area would make it very easy to find that person. And the fact that they are basically on a hit list making them basically targets is very, very serious." *Id*.[6]

The Court then imposed a 240-month sentence—comprised of 180 months for the material support conviction and 60 months for the hacking conviction—and in doing so, noted Ferizi's years-long involvement in hacking:

> Because of the need, among other things, for general deterrence, the need to make sure this defendant is deterred from such future conduct, given his track record

company in exchange for removing the malware. As he said: "When i get money here: lf5Vgj7wMU9ofZWZno9ABsLSQ7XXkLsrG[.] I will make full report for server and method.. i will protect and remove all bugs on your shop!" (ECF No. 2 at 18.)

[6] Another victim impact statement stated thusly: "I have to live constantly under the threat that someone might actually arrive at my residence and harm me or my family members."

> going back five or six years with hacking, the Court is satisfied that a total sentence of 240 months is sufficient but not greater than necessary to achieve the purposes of Section 3553(a).

(ECF No. 77 at 27–28.)

The Court also imposed a 10-year term of supervised release, which included a special condition that Ferizi was "not permitted to have any contact or communications whatsoever with any known terrorist, terrorist organizations, or any known hackers." (*Id*. at 29–30.) The Court also imposed a special condition that Ferizi "satisfactorily participate in such mental health treatment as directed by the probation office with an emphasis on deradicallization." *Id*. at 29.

C. Ferizi moves to amend his sentence

At sentencing, the government mentioned an individual within the Eastern District of Virginia, subsequently identified as Haris Qamar, "who was arrested for … the fact that he drove by the homes of two individuals in Virginia whose names and addresses were on the kill list that Junaid Hussain posted in March of 2015." (ECF No. 77 at 12.) Three days after sentencing, on September 9, 2016, Ferizi moved to amend his sentence under Federal Rule of Criminal Procedure 35(a), arguing that the government's representation improperly suggested that he was the source of the information in Junaid Hussain's March of 2015 "kill list." (ECF No. 72.) In response, the government rejected Ferizi's characterization of its sentencing statement and stressed that it referenced Qamar "to show that persons in the United States actually read and follow ISI[S] kill lists; that these lists are more than just bits and bytes posted on the internet." (ECF No. 74 at 7.)

On October 7, 2016, the Court held a hearing on Ferizi's motion. There, the Court re-explained its sentencing decision by summarizing several letters it had reviewed describing the harm suffered by Ferizi's victims, and cited again a letter from the victim with a unique name:

> I think we had talked about the fact that people with unique names, not like Smith or Brown, where there are just, you know, millions in society, but with a unique name that would make them almost the only person in society, that they are very

> vulnerable to being easily identified when they're on such a list, and this individual, … said, among other things, "I am the only one" -- and this is a quote: "I am the only one with my last name in the country I live in, and it is not difficult at all to find me. There is nothing anyone can do to prevent something happening to me, or worse, to my family, since I would never be able to see or identify anyone. Already, I have had a suspicious visit to my house that I had to report to the [redacted] security, who in turn informed the [redacted] police. These people came to my house and knew my name."

(ECF No. 106 at 3–4.) The Court also explained that the harm suffered by Ferizi's victims originally drove its sentencing decision:

> Now, that is an example … that underscores my conclusion that this kind of conduct is extraordinarily serious and that it does expose innocent people, especially innocent people who are working for the U.S. government or serving in the military, to even if not threats, the fear of threats. It puts people in a, in a position where they are worried, and therefore, it's a very serious crime, and that was the basis upon which this Court felt that a 20-year sentence was appropriate[.]

Id. at 4. The Court then denied Ferizi's motion. *Id*.

D. Ferizi's first motion for compassionate release

On August 7, 2020, Ferizi, then residing at USP Lewisburg, filed a *pro se* motion for compassionate release under 18 U.S.C. § 3582(c)(1)(A)(i). The Court appointed counsel who filed a supplemental memorandum arguing that Ferizi's asthma and obesity were factors placing him at a higher risk of suffering complications should he contract COVID-19. (ECF No. 89.) Given these conditions, Ferizi asked to be released to Kosovo, where he would reside with his family.

The government opposed the motion, in part, due to the seriousness of Ferizi's offense and the government's inability to supervise him in a foreign country. (ECF No. 95.) The government noted that if released, Ferizi would "be entirely outside the jurisdiction of this Court and the supervision of the U.S. Probation Office, free to resume his online activities unmonitored by U.S. law enforcement or the Court." *Id*. at 17. Finally, the government argued that Ferizi's risk of

recidivism was too high to warrant his release and that this risk posed a danger to the community. *Id*.

On October 6, 2020, the Court held a hearing. There, the Court identified several logistical concerns relating to Ferizi returning to Kosovo. The Court then denied Ferizi's motion in light of these logistical obstacles, as well as the government's concerns about its inability to ensure the safety of the community once the defendant left the U.S. As the Court stated:

> I read over the mental health evaluation that was done back in 2016, which was part of, I guess, the sentencing proceeding, and it was interesting that he did voice issues with the United States, and he is, obviously, a fairly skillful hacker. I don't know what kinds of guarantees there could be placed on him that he would not reengage in hacking activities aimed at the United States. If he were being released domestically, I would have ways of controlling him. I could put him on computer monitoring surveillance by the probation office, I could have him on GPS monitoring, I could do all sorts of things, but I can't do that when he's over in Kosovo. And so, the danger that he poses is out there. I'm not saying it's a high risk, but it's certainly not the least risk, and he is mentally unstable based upon the mental health history here. So I have to look at that in terms of the 3553(a) balancing factor because the safety of the community is definitely a factor that goes into any of these types of decisions.

(ECF No. 100 at 9 –10.) The Court reiterated its safety concerns towards the end of the hearing:

> [J]ust in looking at the release plan in place, there's just not an ability to guarantee the safety of the community from any future hacking. I mean, asking the parents to do the monitoring is not the same thing as having a probation officer, it's not the same thing as having access to computers, you know, carefully monitored by a law enforcement agency and then having, you know, monitoring of the computer. We just can't control that.

Id. at 11–12.

E. Ferizi's second motion for compassionate release

On November 11, 2020, Ferizi, now residing at FCI Gilmer, filed a second motion for compassionate release. (ECF No 101.) The crux of Ferizi's renewed motion was that FCI Gilmer was experiencing an outbreak of COVID-19 cases. Ferizi also represented that he had resolved the

practical concerns regarding traveling to Kosovo and that nothing barred his return to his home country. The government opposed the motion, stressing that the changed circumstances did not alter the seriousness of Ferizi's offense or the government's inability to supervise a computer hacker in Kosovo. In the government's view, the 18 U.S.C. § 3553(a) factors "provide[d] the most critical reasons why [Ferizi's] motion should fail." (ECF No. 103 at 1.) As it argued in its opposition,

> Ferizi is a convicted terrorist hacker who seeks to be released to a foreign country, outside the reach of the United States. Despite the updates provided in his new motion, the seriousness of his offense and the danger he poses to the community make him an inappropriate candidate for compassionate release.

Id.

On December 3, 2020, the Court granted Ferizi's motion and reduced his sentence to time served. (ECF No. 105.) In doing so, the Court concluded that Ferizi was particularly susceptible to COVID-19 and had shown a likelihood of contracting the disease in prison.

The Court recognized that Ferizi committed a "serious offense" and that "his actions were harmful to the individuals whose names appeared on the list posted by ISI[S]." *Id*. at 6–7. "Nevertheless," the Court continued, "even defendants who have committed very serious offenses can be appropriately released from custody or supervision where there is no indication that defendant poses a risk to the public, and reducing defendant's sentence to time served will not diminish the seriousness of his offense or respect for the law." *Id*. at 7. The Court then noted that the "defendant's offense did not involve violence, and none of the individuals whose information he gave to ISI[S] suffered physical harm." *Id*. The Court continued as follows:

> Defendant has explained that he "totally and completely oppose[s] ISI[S] and all that it stands for," and that immaturity rather than ideology was the primary motivator of his conduct: "When I gave the information, I was mostly focused on trying to show off my hacking skills to people I had met online. I deeply regret my actions and I accept the consequences of what I have done."

The Court also rejected the government's concerns about recidivism and its inability to supervise Ferizi in a foreign country. In the Court's view, Kosovo would adequately supervise Ferizi.

The Court then reduced Ferizi's sentence to time served and ordered the Bureau of Prisons to place him in a 14-day quarantine, after which he would be released into Immigration and Customs Enforcement custody for deportation to Kosovo.

F. The government appeals and Ferizi is charged with new crimes

On December 15, 2020, the government appealed the Court's release order. (ECF No. 110.) In its opening brief, the government argued that the Court abused its discretion by reaching conclusions at odds with both the factual record and the Court's own prior conclusions. *See* Gov't Opening Br., *United States v. Ferizi*, No. 20-7830 (4th Cir. filed Feb. 9, 2021), ECF No. 17.

On January 8, 2021, while in immigration custody, Ferizi was charged by complaint in the Northern District of California with wire fraud, in violation of 18 U.S.C. § 1343, and aggravated identity theft, in violation of 18 U.S.C. § 1028A. *See United States v. Ferizi*, 3:21-mj-70014, ECF No. 1 (N.D.C.A. Jan. 8, 2021).[7] On January 21, 2021, a grand jury charged Ferizi in a five-count indictment with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; wire fraud, in violation of § 1343; possession of an unauthorized access device, in violation of 18 U.S.C. § 1029(a)(3); transfer of stolen identification documents, in violation of 18 U.S.C. § 1028(a)(2); and aggravated identity theft, in violation of § 1028A. *See United States v. Ferizi*, 3:21-cr-27, ECF No. 4 (N.D.C.A. Jan. 21, 2021).[8] These charges stemmed from Ferizi's conduct in prison while incarcerated on his convictions from the Eastern District of Virginia.

[7] The criminal complaint affidavit is attached to this response as Government Exhibit D.
[8] The indictment is attached to this response as Government Exhibit E.

On November 16, 2021, after hearing oral argument, the Fourth Circuit remanded back to this Court "to consider in the first instance how the new charges, or other relevant evidence revealed since the district court's order of release, impact the discretionary § 3553(a) analysis for compassionate release[.]" *United States v. Ferizi*, No. 20-7830, 2021 WL 5320860 (4th Cir. Nov. 16, 2021). On December 8, 2021, the Court directed the parties to "supplement the record to enable this Court to consider 'how the new charges, or other relevant evidence revealed since the district court's order of release, impact the discretionary § 3553(a) analysis for compassionate release.'" (ECF No. 124.)

Argument

The Court should deny Ferizi's motion for compassionate release.

First, the very basis for Ferizi's motion—that his health conditions present an extraordinary reason for release—has been significantly undercut by his vaccination status. Ferizi, by his own in-court admission, is fully vaccinated with the Moderna vaccine. (Gov. Ex. A at 13 –14.) That fact "precludes a finding that the COVID-19 pandemic presents extraordinary and compelling reasons for his release." *United States v. Kurzynowski*, 17 F.4th 756, 758 (7th Cir. 2021) (citing *United States v. Broadfield*, 5 F.4th 801 (7th Cir. 2021)); *United States v. Traylor*, 16 F.4th 485, 487 (6th Cir. 2021) ("[A] defendant's incarceration during the COVID-19 pandemic—when the defendant has access to the COVID-19 vaccine—does not present an 'extraordinary and compelling reason' warranting a sentence reduction." (quoting *United States v. Lemons*, 15 F.4th 747 (6th Cir. 2021)).

"The underlying arguments for release from prison based on the coronavirus pandemic depend at least on allegations that the risk of contracting COVID-19 in a prison is higher than the risk outside the prison and that the inmate's preexisting medical condition increases that

individual's risk of experiencing a serious, or even fatal, case of COVID-19." *United States v. High*, 997 F.3d 181, 185 (4th Cir. 2021). Because Ferizi's "underlying arguments for release" have been significantly weakened by his vaccination status, releasing him is no longer appropriate.

Second, the new charges in the Northern District of California confirm the government's earlier arguments that Ferizi is too dangerous to release and that granting his motion will not protect the public from further crimes. Given Ferizi's background and history, the new allegations against him are unsurprising.

The defense has repeatedly recognized Ferizi's prior hacking activities. (*See* ECF No. 53 at 7 ("While he had previously engaged in hacking activities and was known to the Kosovar authorities, he was never sentenced for any hacking offenses."), 12 ("As his hacking skills improved, he gained increasing notoriety online."), 13 ("his hacking activities intensified"), 14 ("In 2013, Mr. Ferizi got in trouble for hacking into Kosovo government databases. However, he was given an alternative sentence."); ECF No. 77 at 23 ("Mr. Ferizi has never disputed that he engaged in hacking activities as a youth, as a juvenile, in Kosovo").) Ferizi himself put it best in a letter to the Court: "I have hack[ed] or access[ed] a lot of databases but never got in trouble." (ECF No. 53-2 at 3.)

The Court too has recognized Ferizi's prior hacking activities. The Court did so at sentencing. (*See* ECF No. 77 at 25 ("You obviously have a certain talent for working on the computer. You've been able to hack into Government databases at least since the age of 15."); 28 (noting "the need to make sure this defendant is deterred from such future conduct, given his track record going back five or six years with hacking")). And in denying Ferizi's first motion for compassionate release, the Court characterized him as "a fairly skillful hacker" and doubted

whether it could prevent him from engaging in "hacking activities aimed at the United States." (ECF No. 100 at 9.)

The new charges in the Northern District of California only reaffirm the obvious. Ferizi is a hacker and a fraudster, and he has no qualms about victimizing innocent people to benefit himself.

According to the criminal complaint affidavit, on October 3, 2017, while incarcerated in the Federal Correctional Institute in Terre Haute, Indiana Ferizi emailed his brother in Kosovo and asked him to keep his email accounts alive. He provided his brother with the arditferizi95@gmail.com address and password as well as five other accounts and passwords. (Complaint ¶ 15.) On February 26, 2018, Ferizi spoke with his brother, who confirmed having accessed the accounts. *Id*. at ¶ 16. Search warrant returns indicate that the previous day, "files were prepared to be downloaded from the arditferizi95@gmail.com e-mail account that included large databases of stolen PII." *Id*. at ¶ 17. "The databases included extensive lists of stolen e-mail accounts, partial credit card numbers, passwords, and other PII." *Id*. These databases are believed to be "the fruits of [Ferizi's] previous criminal hacking activity." *Id*. Search warrant returns indicate that several large databases of stolen PII were prepared for downloading via the Google Takeout tool, which allows users to download their emails and the contents of their Google Drive. On February 25, 2018, the arditferizi95@gmail.com address received an email indicating that the data was ready for downloading. Within the Takeout files were "large databases of stolen PII, were available for download or about February 25, 2018[.]" *Id*. at ¶ 45. The Google Takeout tool must be initiated by someone. It does not occur on its own. *Id*.

Among the sets of data contained in Ferizi's email account was a spreadsheet in a folder tilted "hehe" that contained 51 rows of what appeared to be stolen PII from Macy's customers,

including email addresses, passwords, and partial credit numbers. *Id*. at ¶ 47. The FBI interviewed three individuals named on the Macy's spreadsheet. All three confirmed they had accounts with Macy's and had been victimized by other instances of identity theft. *Id*. at ¶ 48. One victim reported that she no longer uses the email address listed on the Macy's spreadsheet and believed she was hacked about three years prior due to suspicious activity. *Id*. at ¶ 49. The victim further "advised that she experienced high levels of credit card fraud over the past four to five years and that she normally has to change her credit card numbers three to four times a year due to fraud." *Id*.

Another database located in Ferizi's Google Drive was called "#opisrael" and "contained first name, last name, e-mail address, phone number, ID number, and address data for what appeared to be more than 17,000 victims." *Id*. at ¶ 50. Op Israel refers to an annual coordinated cyber-attack where hacktivists target Israeli government websites and Israeli citizens. *Id*. Another database contained a spreadsheet with 55 email addresses and passwords. *Id*. at ¶ 51. And a final database called "USA-Emails-Clean" contained 438,334 rows of email addresses. *Id*. at ¶ 52. Within this database were government email addresses ending in "usdoj.gov", "hq.doe.gov", "sanantonio.gov", "flsenate.gov", "sec.gov", "gsa.gov", and "noaa.gov." *Id*. Search warrant returns for Ferizi's Facebook account also revealed that he previously sent himself a list of the 100,001 rows of email addresses and password he stole from the victim company in this case. *Id*. at ¶ 55.

The FBI also learned through an inmate housed at Terre Haute ("MI") that Ferizi was "cashing out" from his crimes and using his family members to do so. *Id*. at ¶ 25. On December 27, 2017, MI spoke to an identified female ("FI"). FI told MI that she had sent "those emails." *Id*. MI warned FI not to get involved with Ferizi because he was engaging in illicit activity. *Id*. FI responded that she wished she had known this information before she had emailed Ferizi's brother.

Id. The FBI later interviewed FI concerning her conversation with MI. *Id*. at ¶ 28. FI searched her emails for the name of Ferizi's brother and identified messages beginning around October 2017. FI relayed that she had been requested to open bitcoin accounts for Ferizi and his brother. *Id*. FI believed that Ferizi and his brother discussed her opening Blockchain, Bitflyer, and Coinbase bitcoin accounts. *Id*. She also advised that her emails with Ferizi's brother took place from approximately October 2017 to January 2018. *Id*.

The day after the interview, FI provided the FBI an email she had sent Ferizi's brother on December 27, 2017. *Id*. at ¶ 30. The email provided as follows:

> I have been told to send you an email from the address to which you can send the user name and password for certain escrow accounts and then the escrow account information itself for the various accounts. Please send this information to the email from which this being sent.

Id.

The FBI also interviewed MI. *Id*. at ¶ 32. MI relayed that Ferizi possessed a white iPhone while incarcerated and that he wanted MI to pass information to FI regarding email accounts that contained bitcoin so that she could relay it to Ferizi's brother. *Id*. MI also relayed the Ferizi associated in prison with a convicted perpetrator of the 1993 World Trade Center Bombing and that he saw "terroristic material and severed heads" on Ferizi's phone. *Id*. at ¶¶ 32, 38. The FBI also learned that Ferizi lost his email privileges around December 13, 2017. *Id*. at ¶ 34.[9]

Separate and apart from Ferizi's most recent scheme, the criminal complaint also details two other instances of Ferizi discussing or engaging in other unlawful ventures with innocent persons' PII. For example, in 2015 Ferizi and his brother discussed how best to capitalize on a recent data breach of the Ashley Madison website. *Id*. at ¶ 53. The complaint also alleges that in

[9] Several months before losing his email privileges, Ferizi emailed DIPVTEL expressing interest in obtaining a virtual phone number in prison. (*See* Gov. Ex. F.)

2016, Ferizi discussed with law enforcement how an identified fellow hacker would use "account checkers" to mine for stolen data from eBay, PayPal, and financial websites. *Id*. at ¶ 62. An "account checker allows a hacker, in a quick and automated way, to identify if a group of stolen login credentials from one website can be repurposed to unlawfully access the account of the same victims on other websites . . . based on the common practice of individuals using the same email and password for multiple web sites." *Id*. at ¶ 64. A review of Ferizi's Facebook account revealed private message between Ferizi and the identified hacker displaying their use of account checkers in August 2015. *Id*. at ¶ 63. The FBI also identified private messages between Ferizi and the identified hacker demonstrating their use of account checkers on a victim's stolen login credentials approximately 17 times between July and August 2015. *Id*. at ¶ 65.

As part of the investigation in the Northern District of California, the government has obtained a police report from Kosovo detailing six criminal investigations initiated into Ferizi's conduct. (*See* Gov. Ex. B.)[10] A brief synopsis of each case follows:

1. 2012-DHKO-002 Article 264 (Accessing computer systems): Ferizi is alleged to have attacked various online platforms, "including the government network, customs, PTK [Post and Telecommunications of Kosovo], RTK [Radio Television of Kosovo]," among others. The suspects accessed the aforementioned systems and extracted sensitive PII which they later publicized online. Ferizi also hacked into an online media portal and posted fake news about the Prime Minister of Kosovo.[11]
2. 2012-AD-3253 Article 264 (Accessing computer systems): Ferizi was arrested and released on the same day. No other details are available.
3. 2012-DB-1241 Article 264 (Accessing computer systems): Ferizi is alleged to have attacked several different websites, interrupting their functioning.
4. 2013-YI-2 Article 374 (Ownership, control or unauthorized possession of weapons" and Article 339 (Accessing computer systems): In 2013, Kosovo Customs intercepted a package sent to Ferizi from Israel containing a bulletproof vest, two helmets, two handles for long weapons, two holsters for short weapons, and two "two protective sets for hands for [an] AK-47."

[10] Government Exhibit C is the same report in the original Albanian.

[11] This is likely the same prosecution discussed in the forensic psychological evaluation. (Report at 5.)

5. 2013-DKKO-026 Article 339 (Accessing computer systems) and Article 417 (Impersonating a public official): In 2013, Ferizi is alleged to have created a fake social media account for Vlora Citaku, a Kosovo Minister. Ferizi then used this account to make fraudulent posts under Citaku's name. Authorities arrested Ferizi for 24 hours and seized his passport.
6. 013-DKKO-010 Article 339 (Accessing computer systems): Ferizi is alleged to have attacked the Telegrafi webpage and caused it to cease functioning. During the attack, the Telegrafi official email address received the following message: "Respect the Islamic faith or the Islamic faith punishes you."

The police report also explains how Ferizi managed to leave Kosovo for Malaysia in 2015. As noted above, Kosovo authorities seized Ferizi's passport in 2013. Shortly after, Ferizi appeared at the Gjakova police station and reported his passport lost. (Gov. Ex. B at 5.) The Gjakova police issued Ferizi a certificate for a lost document, which he then used to successfully apply for a new passport. In essence, Ferizi fraudulently obtained a genuine passport.

* * *

All this conduct paints a familiar picture. Prior to this prosecution, Ferizi had prior run-ins with Kosovo authorities for hacking activities. At one point, he received an alternate sentence. Clearly, that bit of good fortune did little to deter him from reoffending. Ferizi then committed the offenses involved in this case. Once again, he found himself accused of breaching systems and stealing PII. This time, however, he decided to aid ISIS in the process. But this was not his first time doing so. Prior to sending Junaid Hussain the PII of 1,300 victims, Ferizi sent Tariq Hamayun, another ISIS member, credit card information belonging to 68 other individuals. In 2016, the Court imposed a sentence that not only fit the crime but also the criminal. Prior to sentencing in 2016, Ferizi wrote to the Court. He stated that "I respect this country and its laws. (ECF No. 53-2 at 5–6). He also stated that "i know that I won't do anything like this never." *Id* at 6. But a little over one year later, Ferizi picked up exactly where he left off. Once again, Ferizi is accused of engaging

in a fraudulent scheme to capitalize on innocent persons' PII. And again, Ferizi has used deception to circumvent the authorities and accomplish his goals.

Ferizi will likely argue that the new charges are only allegations and that they have not yet been proven beyond a reasonable doubt. But while technically true, Ferizi is now under indictment, which itself "'conclusively determines the existence of probable cause' to believe the defendant perpetrated the offense alleged." *Kaley v. United States*, 571 U.S. 320, 328 (2014) (quoting *Gerstein v. Pugh*, 420 U.S. 103 (1975)). And even if Ferizi is acquitted of the new charges, the bare facts constituting his new offense conduct will remain, and the Court can still consider those facts in the compassionate release setting. *See United States v. Watts*, 519 U.S. 148 (1997); *United States v. Grubbs*, 585 F.3d 793, 799 (4th Cir. 2009) ("[A] sentencing court may consider uncharged and acquitted conduct in determining a sentence, as long as that conduct is proven by a preponderance of the evidence."); *United States v. Jones*, 31 F.3d 1304, 1316 (4th Cir. 1994) (a "defendant need not be convicted of the charges constituting relevant conduct for him still to be held accountable for them" when a sentencing court determines the defendant's sentence, as long as the government "establish[es] the existence of these other incidents by a preponderance of the evidence").

The conduct forming the basis for the new criminal charges consists of Ferizi asking his brother to maintain email accounts containing databases with information on hundreds of thousands of people, using an intermediary in prison to communicate with his coconspirator brother in Kosovo, and likely doing so to circumvent restrictions on his communications. At its core, this is all familiar conduct. The same defendant, more stolen PII, and more deception. It is also now apparent that Ferizi hoodwinked Kosovo authorities to obtain a new passport after they had seized his. Still more deception.

Prior to sentencing in 2016, Ferizi wrote to the Court that he "deeply regret[ed] [his] actions" and "accept[ed] the consequences of what [he] ha[d] done." PSR ¶ 27. But when Ferizi made substantially the same claim at sentencing, *see* ECF No. 77 at 24–25 ("I feel so bad for what I did. I take full responsibility for that."), the Court asked if he had "any true understanding of what [he] actually did[.]" (ECF No. 77 at 25.). When Ferizi responded that he did, the Court responded that it was "still not sure." *Id*. And when Ferizi attempted to justify his actions, the Court rejected his excuses. *Id*. The Court's original inclination was correct. And Ferizi cannot now demonstrate otherwise. *See United States v. Sherwood*, 986 F.3d 951, 954 (6th Cir. 2021) ("[W]e presume that the district court's initial balancing of the § 3553(a) factors during Sherwood's sentencing remains an accurate assessment as to whether those factors justify a sentence reduction, meaning Sherwood must make a compelling case as to why the sentencing court's § 3553(a) analysis would be different if conducted today."); *see also United States v. Keitt*, — F.4th —, 2021 WL 6058144, at *4 (2d Cir. Dec. 22, 2021) ("Indeed, it would have been most unusual if the district court's analysis of the § 3553(a) factors had been markedly different after such a short period of time."). "[T]he burden falls on" Ferizi "to convince [this Court] to exercise discretion to grant the motion after considering the [Section] 3553(a) factors." *Ward v. United States*, 11 F.4th 354, 361 (5th Cir. 2021) (cleaned up) (citing *United States v. Shkambi*, 993 F.3d 388, 392 (5th Cir. 2021)). And although the government maintains that Ferizi never merited compassionate release, whatever doubt might have existed should now be extinguished by his conduct in prison.

At the height of the Pandemic, Ferizi sought compassionate release from the Court. He initially asserted that "[t]he punishment he has already endured is more than sufficient to deter him from ever re-offending." (ECF No. 89 at 4.) Not so. In a subsequent motion, Ferizi argued that he "ha[d] matured, stabilized, and outgrown the juvenile impulses that caused him to commit his

offense. Likewise, he has been sufficiently deterred from ever engaging in this type of conduct again." (ECF No. 101 at 2.) Once again, more empty words. A defendant who commits an offense soon after completing his prison sentence does not merit compassionate release. *See High*, 997 F.3d at 189. That principle applies doubly to defendants who commit crimes *while incarcerated* on the offense from which they seek early release. *Accord United States v. Ventura*, 864 F.3d 301, 313 (4th Cir. 2017) (affirming court's imposition of same sentence despite prior vacatur of conviction and holding that "court did not err in taking account of [defendant's] misdeeds while he was in custody with the BOP.").[12]

Ferizi was too dangerous to release even before the new charges. His background paints a clear and consistent portrait of an individual thoroughly consumed by the enterprise of hacking. He is the self-proclaimed leader of a Kosovo hacking group that claims to have compromised over 20,000 websites. PSR ¶ 10. Ferizi believes hacking is morally justified and has admitted that it gives him a sense of control and power that he likes. He has had repeated, similar run-ins with Kosovo authorities for hacking activities and previously committed a crime remarkably similar to the instant offense. He has, in his own words, "hack[ed] or access[ed] a lot of databases[.] (ECF No. 53-2 at 3.) When he breached the victim company's server in this case, he toyed with, threatened, and attempted to extort a ransom in bitcoin from his victim. Given his history, and the

[12] Ferizi previously cited his prison courses and completion of a GED as evidence of his maturation. (*See* ECF No. 89 at 18; ECF No. 96 at 9.) But the significance of this coursework is unclear at best. As a general matter, taking courses and completing a GED is relatively common in federal prison. *See United States v. Hunter*, 12 F.4th 555, 572 n.10 (6th Cir. 2021). And more importantly, Ferizi already had a high school diploma when he committed the crime, *see* PSR ¶ 59. Moreover, he was literally enrolled in a university (having completed approximately 22 credits) at the time he committed his initial offense. PSR ¶ 70. Other than simply asserting that his coursework was evidence of maturation and rehabilitation, Ferizi never explained why having a second high school diploma would have any bearing on his likelihood of recidivating. At bottom, there is simply no reason to elevate Ferizi's specific coursework beyond what the record supports.

fact that "the risk of recidivism is inversely related to an inmate's age at release[,]" *United States v. Fowler*, 948 F.3d 663, 670 (4th Cir. 2020) (internal quotation marks and citation omitted), there is every reason to believe Ferizi will continue to ply his trade if released to Kosovo.[13] "Sending [Ferizi] overseas will not guarantee the safety of people in this nation or any other." *United States v. Ugbah*, 4 F.4th 595, 597–98 (7th Cir. 2021) (affirming denial of compassionate release to non-citizen on-line fraudster because "[t]he Internet reaches across the globe, and [he] became involved in online fraud while in Nigeria."). The new charges simply confirm that reality.

Finally, releasing Ferizi five years into a twenty-year sentence would not reflect the seriousness of the offense, promote respect for the law, provide adequate deterrence, or provide just punishment.

Ferizi's offenses caused immense and lasting harm to his victims. The Court has repeatedly recognized the seriousness of Ferizi's crimes. The passage of time has done nothing to offset the objective seriousness of the offense, or the harm suffered by Ferizi's victims. Indeed, the FBI continues to work with private entities to remove Ferizi's kill list whenever it surfaces on the internet. "There are crimes whose consequences vividly outlive the criminal act." *United States v. Friend*, 2 F.4th 369, 382 (4th Cir. 2021). This is such a case.

The Court may also consider the amount of time Ferizi has already served. *See United States v. Kibble*, 992 F.3d 326, 331 (4th Cir. 2021). Releasing Ferizi at this juncture would unduly

[13] As the government argued previously, a defendant's pattern risk score does not account for numerous defendant-specific factors, such as the seriousness of the offense of conviction, a defendant's ideology, or the inability to supervise a defendant after release. (ECF No. 95 at 20.) Critically, a PATTERN risk score does not account for a defendant like Ferizi's unique skillset. Thus, in many cases a PATTERN risk score will not be an adequate means for gauging a defendant's risk of recidivism. *See United States v. Bass*, 17 F.4th 629, 640 (6th Cir. 2021) (reversing grant of compassionate release where court relied on defendant "reportedly 'low' PATTERN score as proof that [he] was at low risk of reoffending upon release."). And of course, the best evidence of that is this very case.

minimize the severity of his offense. Releasing Ferizi would also undermine respect for the law. And while that is true as a general matter, it is especially so here, where Ferizi—who has previously feigned respect for this country's laws—is currently under indictment in another district. Moreover, releasing Ferizi would fail to afford adequate deterrence. Even without the new charges, a 75% decrease in sentence fails to afford any deterrent value. But again, that is doubly so here, where the defendant is a young, skillful hacker who currently stands accused of committing new crimes involving the theft of PII. Some defendants reoffend after being released. Ferizi could not wait that long. Releasing him to Kosovo to rejoin his brother and co-conspirator is a recipe for disaster.

The compassionate-release statute is a "mechanism for lenity." *United States v. Brooker*, 976 F.3d 228, 231 (2d Cir. 2020); *accord Dillon v. United States*, 560 U.S. 817, 828 (2010) ("[18 U.S.C.] § 3582(c)(2) represents a congressional act of lenity"). To secure such lenity, a defendant must first "meet the heightened standard of 'extraordinary and compelling' reasons[.]" *United States v. McCoy*, 981 F.3d 271, 287 (4th Cir. 2020). In light of recent developments, Ferizi cannot meet that heightened standard. And even if he had, "a district court may not grant a sentence reduction under 18 U.S.C. § 3582(c)(1)(A) without 'considering the factors set forth in section 3553(a) to the extent that they are applicable.'" *Kibble*, 992 F.3d at 331 (4th Cir. 2021). Here, the sentencing factors weigh uniformly against release. Because Ferizi cannot satisfy any of the statutory prerequisites for release, the Court should deny his motion.

Conclusion

The Court should deny Ferizi's motion for compassionate release.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/

Danya E. Atiyeh
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
Office: (703) 299-3700
Email: danya.atiyeh@usdoj.gov

/s/

Joseph Attias
Assistant United States Attorney
United States Attorney's Office
919 East Main Street, Suite 1900
Richmond, Virginia 23219
Office: (804) 819-5400
Email: joseph.attias2@usdoj.gov

Certificate of Service

I hereby certify that on December 22, 2021, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

By: /s/

Joseph Attias
Assistant United States Attorney